To: All Field Offices From: NSD/CID
(U) Re: ~~(S)~~ 288-HQ-1242560, 02/09/1998

Referral/Consult

[redacted]

(U) ~~(S)~~ DNS servers provide users with hostname to Internet Protocol (IP) address conversions and are critical pieces of the overall network infrastructure. Loss of functionality of a DNS server would have resulted in loss of the bases ability to communicate electronically with the outside world. An intruder could also alter the servers address tables, allowing the intruder to assume the identity of a registered site or redirect traffic to an alternate site of the intruders choosing.

[redacted]

Referral/Consult

To: All Field Offices From: NSD/CID
(U) Re: (S) 288-HQ-1242560, 02/09/1998

Referral/Consult

(U) (S) The intruder(s) made use of University systems and commercial ISP's to facilitate entrance into the targeted systems and to transfer captured files. These originating sites include:

Boston, MA:
Boston University
Harvard University
Massachusetts Institute of Technology

New Haven, CT
Yale University
University of Connecticut
Iconnects (a commercial ISP)

Maryland
University of Maryland
Clark.net(ISP)

Seattle, Washington
Washington University

Indiana
Notre Dame University

To: All Field Offices From: NSD/CID
(U) Re: ~~(S)~~ 288-HQ-1242560, 02/09/1998

Utah
Utah State University

Referral/Consult

(U) ~~X~~

(U) ~~(S)~~ The motive for these attacks is not known. There has been speculation that the intrusions may be part of an ongoing game of "capture the flag" currently being played out by a Dutch hacker group, across IRC channels. There is also concern that these intrusions may be related to current U.S. military activities in the Persian Gulf.

(U) ~~(S)~~ Leads to field offices will be forthcoming. It is requested that CITA team members be prepared to cover leads in an expeditious manner.

♦♦